

REMARKS

Applicants respectfully request reconsideration of the rejection of this application as examined pursuant to the office action of June 12, 2008. In the office action, an amendment made to the Specification and Claims 41-58 were examined. The Specification was objected to based on an assertion that it disclosed information deemed to be new matter. Claims 41-58 were rejected under 35 USC § 112, first paragraph, as failing to comply with the written description requirement. Claims 41-58 were also rejected under 35 USC § 103(a) as being unpatentable over US published application Publication No. US2005/0273600 of Seeman ("Seeman") in view of US Patent No. 6,502,131 issued to Vaid et al. ("Vaid"). Claims 41-58 remain pending.

Paragraph (19) of the Specification has been amended to remove reference to the packet forwarding device clarification, although Applicants respectfully submit that those of skill in the art will readily recognize that the forwarding devices described throughout the Specification are packet forwarding devices. Nevertheless, for purposes of expediting the examination of this Application, the reference to packet forwarding devices has been removed from paragraph (19) of the Specification. The reference to packet forwarding devices has also been removed from amended Claims 41, 50, 51, 54, 56 and 57. As a result of these amendments, Applicants respectfully suggest that the objection to the Specification and the 35 USC § 112, first paragraph, rejection of Claims 41-58 have been successfully traversed. Withdrawal of that objection and that rejection is therefore requested.

Applicants have amended independent Claims 41 and 54 to make clear that the changing of static and/or dynamic policies for an attached function occur at a central switching device of the network infrastructure and not at a server. The independent claims have also been amended to make clear that the trigger that may result in the implementation of one or more policy changes include triggers that are not related to information acquired about the attached function itself. The prior art has always been to evaluate conditions, make determinations and implement modifications through the network administrator-controlled server. The interconnection devices of the network, such as routers, network entry devices and central switching devices, have only implemented instructions. The present invention substantially speeds up the effectiveness of maintaining network security by implementing analysis, decision making and change instructions much closer to the attached function at the interconnection devices of the network. Claims 41 and 54 have been amended to state specifically that the central switching device

makes decisions on policy changes based on trigger information and also implements those policy changes. The cited art fails to provide such process steps as they are directed to server-only controlled security. Applicants respectfully submit that the amendments made to the independent claims clearly distinguish the present invention from the cited art. Applicants note that the claim amendments are fully supported by the original Specification at least at paragraphs (10), (19) and (20).

The 35 USC § 103(a) Rejection

Claims 41-58 were rejected in the June 12, 2008, office action as being unpatentable over Seeman in view of Vaid. Applicants respectfully submit that the Seeman reference is inapplicable to the present invention, particularly in view of the amendments made to independent Claims 41 and 54. Specifically, the Seeman reference is directed to a system completely controlled centrally in a server for the purpose of digital rights management. Such a system does not contemplate any form of information transfer that involves decision making anywhere other than at the central management server. All aspects of the Seeman reference are directed to ensuring the user has the permitted access to the information in the server. Nowhere does Seeman suggest that policy information or policy changes for a user are to be contained in a central switching device. The present invention is directed to regulating network access, but allows for that regulation to take place in a much more localized manner substantially closer to the attached function and, therefore, more likely to provide effective network security in a fine-tuned manner. As a result, a failure or security event in one region of a network system is much less likely to induce a complete system-wide failure. On the other hand, the Seeman system, with central control only of policy history storage and modification, is more prone to system-wide failure.

It is stated in subparagraph g on page 4 of the June 12, 2008, office action that Seeman teaches a method including the step of “monitoring the network usage for triggers,” citing the abstract and paragraph [0021] of the reference. The Seeman abstract states:

A computer data security system, including a file parser for determining if a computer file contains protected data, a file decrypter for decrypting encoded files, a file encrypter for re-encoding decrypted files that have been modified, a rights processor for determining data usage rights for a process that has been launched, the data usage rights restricting the process by limiting permissible data access commands that can be issued by the process, and a process monitor for

monitoring processes within a computer, including a command interceptor for intercepting a data access command issued by the process, and a command blocker for blocking the intercepted command if the intercepted command accesses protected data, and if the data usage rights indicate that the command is not permissible. A method is also described and claimed.

Paragraph [0021] of Seeman states:

The present invention uses client-side software to decrypt protected information, enforce the usage rights associated with the information, monitor the flow of protected information across the end-user's machine (where permitted), and subsequently encrypt protected information when it is saved. It also uses a server computer to provide de/encryption keys, usage rights, and data lists for clients. It also uses an administration tool for managing the above server-based information.

As noted, Seeman is directed to digital rights management. The monitoring described in the abstract and paragraph [0021] is limited in its focus to either blocking a command associated with providing access to specific data by the particular data requestor (read: attached function), or reviewing the flow of the requested information across the end-user's machine (read: attached function). In both instances, the monitoring is related to the specific data sought by the particular attached function or the usage of that specific information sought by that particular attached function. The present invention, on the other hand, monitors for an array of triggers, some of which may be unrelated to the information or actions of the attached function gaining access to network services. Seeman fails to teach such a process. The amended independent claims of the present Application describe that process.

It is stated in subparagraph h on page 4 of the June 12, 2008, office action that Seeman teaches a method including the step of "modifying for the attached function one or more of the policies upon detection of one or more triggers" citing paragraph [0023] of the reference.

Paragraph [0023] of Seeman states

There is further provided in accordance with a preferred embodiment of the present invention a method for computer data security, including determining if a computer file contains protected data, decrypting encoded files, re-encoding decrypted files that have been modified, determining data usage rights for a process upon launch of the process, the data usage rights restricting the process by limiting permissible data access commands that can be issued by the process, intercepting a data access command issued by the process, and blocking the intercepted command if the intercepted command accesses protected data, and if the data usage rights indicate that the command is not permissible.

It can be seen that the Seeman reference is focused only on data rights management. That is, Seeman relates to information security. On the other hand, the present invention is directed to the much more complex and difficult goal of network security. Seeman describes steps for preventing unauthorized exchange of specific data and therefore modifies the data itself. The present invention is directed to actions of the attached function or events associated with the entire network, makes a determination whether policies associated with that attached function's access to the range of network services must be modified, and which occurs at a central switching device of the network infrastructure. That is, at a location more proximate to the attached function. The cited passage of Seeman, and Seeman in general, fails to describe network access control of any type. Seeman also fails to describe data rights management functions performed at an interconnection device rather than a server. The amended independent claims of the present Application describe such a process implemented through the central switching device.

The amendments made to the independent claims make even clearer that Seeman fails to describe a network security method of the type provided by the present invention.

Applicants further note that additional features of the methods of the present invention described in certain dependent claims that are asserted in the June 12, 2008, office action as being disclosed by Seeman are not taught by Seeman.

First, in the third full paragraph on page 6 of the June 12, 2008, office action it is stated "Regarding claim 48, Seeman teaches the method as claimed in Claim 41 further comprising the step saving set and modified policies associated with the attached function as the stored policy history for the attached function," citing paragraph [0019] of Seeman. Paragraph [0019] of Seeman states:

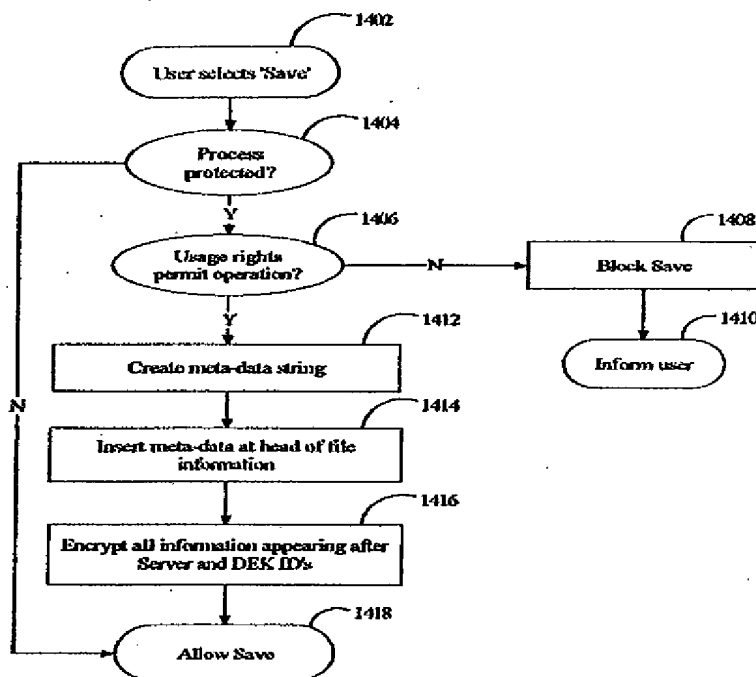
The present invention provides a method and system for protecting digital documents from unauthorized dissemination, while enabling a practically unlimited range of usage options. The invention is distinguished from prior art in a number of respects. The first distinction is that the invention decouples usage constraints from the protection mechanism; rather than applying usage constraints, the invention uses as its protection benchmark the principle that protected information must not reach unauthorized users in usable form. Thus, activities on the part of the user that do not violate this principle, such as editing, copying, and pasting of information, can be permitted. The protection mechanism tracks the flow of protected information, ensuring that the protection attribute

'sticks to' the information--such that it is subsequently stored and transmitted in protected format. This capability, which is generic to any Windows file format, enables the protection of data that previously could never be effectively secured via existing DRM technologies, e.g. source code.

The cited passage from the Seeman reference describes the complete scope of the concept of data rights management for which patent protection is sought. That passage fails to describe anything about the control of access to network services by an attached function, which access is determined at a central switching device, and which is the focus of the present invention. Moreover, paragraph [0019] of Seeman fails to make any mention of network policies. Instead, it is directed to singing the praises of making "sticky" data. That is, coupling attributes of protection to data that may (or may not) be transmitted. The present invention described by dependent Claim 48 relates to storing policies associated with the attached function, not with transmittable data.

Second, in the next-to-last paragraph on page 6 of the June 12, 2008, office action it is stated "Regarding claim 49, Seeman teaches the method as claimed in Claim 48 further comprising the step establishing rules of hierarchy for saved set and modified policies," citing Figure 14 of Seeman. Figure 14 of Seeman is:

Figure 14. Saving Protected Data



A careful review of Seeman Figure 14 shows that it makes no reference to establishing hierarchy for saved set or modified policies. The text associated with the description of Seeman's Figure 14 confirms this omission. Specifically, paragraphs [0231] to [0234] of Seeman are directed to saving protected data, stating as follows:

14. Saving Protected Data

Reference is now made to FIG. 14, which is a simplified flowchart of a method for saving protected information to disk, in accordance with a preferred embodiment of the present invention. At step 1402, the user selects 'Save' for process/window information, or Windows attempts to automatically save the information to a temporary file on disk. The Client's process monitor then intercepts the underlying Windows function call, e.g. 'WriteFile' where the file is being saved to the local computer, or 'WriteStream' where the file is being saved to a remote computer. At step 1404 the process monitor consults the protected processes whiteboard in order to determine whether the process which made the call is protected. If it is not, the process monitor skips to step 1418. If the process is protected, at step 1406 the process monitor consults the whiteboard to determine whether the usage rights designated for this process allow saving of information to disk. If saving is not allowed--e.g., the process is designated as 'read-only'--at step 1408 the process monitor aborts the save operation, and at step 1410 displays an error dialog to the user.

If saving is allowed, at step 1412 the process monitor invokes the Client's encrypter, which accesses the whiteboard record corresponding to the process in question. The encrypter then compiles a meta-data string by concatenating the information in the record's 'Server', 'encrypting DEK', and 'meta-data' fields, and inserts 'start' and 'end' flags at the beginning and at the end of the string. At step 1414 the encrypter inserts the meta-data string at the head of the target information. At step 1416 the encrypter retrieves the DEK specified in the 'encrypting DEK' field from the DEK list associated with the specified Server in the Client's access/usage properties list. The encrypter then encrypts the meta-data appearing after the 'start' flag, Server ID and DEK ID values, and the file information itself.

At step 1418, the process monitor passes the information to the calling function, allowing it to be saved to disk.

Nowhere can it be seen in the cited Seeman figure or the corresponding text that Seeman teaches anything about establishing rules of hierarchy for saved set and modified policies for an attached function. Instead, as it consistently does throughout the document, Seeman is focused on data rights management including, with respect to Figure 14, limiting the capability of a user to save the data. Seeman teaches the processes of determining whether to allow the user to copy the data to a disk and, if that permission is granted, the process for encrypting that data. Nowhere does Seeman teach or fairly suggest establishing rules of hierarchy for saved set and

stored policies for an attached function's access to network services as is described in pending dependent Claim 49 and in independent Claim 54.

Third, in the paragraph extending from the bottom of page 6 to the top of page 7 of the June 12, 2008, office action it is stated "Regarding claim 50, Seeman teaches the method as claimed in Claim 49 wherein a portion of the saved set and modified policies are stored on a local network infrastructure device to which the attached function is directly connected and a remainder of the saved set and modified policies are stored on a central network infrastructure device to which the attached function is not directly connected," citing Figure 14 of Seeman.

A review of Figure 14 and the associated paragraphs of Seeman incorporated above indicates that Seeman fails to make any mention of the storage of network usage policies for an attached function, let alone distinguishing whether to store some policy information on one device and the remainder on another device. Seeman does not make any mention in the noted portions of that reference of doing so even with respect to protected data. Instead, Seeman appears to describe the option of saving protected data to a disk or to a computer, not dividing that information between the disk and the computer. Presently pending dependent Claims 50 and 56 describe this feature of the present invention, which is clearly distinguished from what Seeman teaches.

Fourth, in the first full paragraph on page 7 of the June 12, 2008, office action it is stated that "Regarding claim 51, Seeman teaches the method as claimed in Claim 50 further comprising the step of overriding saved set and modified policies stored on the centrally located network infrastructure device with saved set and modified policies stored on the local network infrastructure device," citing Figure 14 of Seeman.

Again, Seeman simply does not describe anything about modifying policies associated with access by an attached function to network services, and does not do so with respect to making decisions regarding policy modifications at a central switching device. A review of Figure 14 and the associated text of Seeman confirm that Seeman is silent about overriding saved set and modified policies stored on the server with saved set and modified policies stored on the central switching device. Presently pending dependent Claims 51 and 57 describe this feature of the present invention, which is clearly distinguished from what Seeman teaches.

Fifth, in the second full paragraph on page 7 of the June 12, 2008, office action it is stated that "Regarding claim 52, Seeman teaches the method as claimed in Claim 48 further comprising

the step of invalidating the saved set and modified policies upon the occurrence of a specified event,” citing Figure 14 of Seeman.

Seeman fails to describe anything about modifying policies associated with access by an attached function to network services, and does not do so with respect to making decisions regarding policy modifications at a central switching device. A review of Figure 14 and the associated text of Seeman confirm that Seeman is silent about invalidating the saved set and modified policies upon the occurrence of a specified event. Presently pending dependent Claims 52 and 58 describe this feature of the present invention, which is clearly distinguished from what Seeman teaches.

Finally, in the third full paragraph on page 7 of the June 12, 2008, office action it is stated that “Regarding claim 53, Seeman teaches the method as claimed in Claim 41 wherein the only static policy is that there is a dynamic policy,” citing paragraph [0016] of Seeman. Paragraph [0016] of Seeman states:

In all the above cases, the information in question could be highly sensitive, yet there may be no centralized mechanism to monitor such information--especially while it is still ‘work in progress’ that is distributed in peer-to-peer fashion; and that information must be in malleable form such that it can readily be reworked, rather than fossilized in a static or semi-static format, for collaboration to be truly effective. This in fact represents the typical state of affairs in the corporate workplace--yet it is precisely there that existing DRM technologies fail.

This portion of the Seeman reference identifies a limitation associated with digital rights management, but is silent with respect to network security. The present invention is directed to network security and dependent Claim 53 describes a policy modification method for an attached function seeking access to network services and further describes a version of that method wherein there are only dynamic policies. The cited passage of the Seeman reference used in rejecting dependent Claim 53 fails to make any type of distinction with respect to static and dynamic policies. The passage includes the word “static,” but fails to use it in relation to network access policies. Instead, the cited passage is directed to the form of the information (data) that is to be transferred. Again, Seeman is consistent throughout in being limited in focus to data rights management. The present invention described in dependent Claim 53 is clearly distinct from anything taught by Seeman.

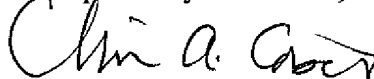
In regard to the Vaid reference, Applicants note that Vaid appears to be focused on the concept of graphical user interface arrangements. The present invention is directed to evaluating policy conditions for an attached function seeking access to network services, modifying policies based on triggers that may or may not be related to the attached function, and carrying out that modification based on decisions made at a central switching device connected to the attached function.

Applicants respectfully submit that the combination of Seeman and Vaid fails to describe the present invention as defined by the amended claims. For this reason, Applicants respectfully suggests that the 35 USC § 103(a) rejection of pending Claims 41-58 has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

Applicants respectfully suggest that the amendments made to the Specification and claims and the arguments presented herein fully address the objection to the Specification and the rejections under 35 USC §§ 112, first paragraph, and 103(a). Allowance of pending Claims 41-58 is therefore requested. Applicants note that by this amendment, no new claims have been added. Therefore, no additional filing fee is required.


Respectfully submitted,



Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicants
Verrill Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530

Certificate of Transmission

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450, on September 11, 2008, using the EFS-Web service. It is hereby requested that this filing be granted a filing date of September 11, 2008.


Chris A. Caseiro